2007-03

Bridging the gap in port security : network centric theory applied to public/private collaboration

Wright, Candice L.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3610

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BRIDGING THE GAP IN PORT SECURITY; NETWORK CENTRIC THEORY APPLIED TO PUBLIC/PRIVATE COLLABORATION

by

Candice L. Wright

March 2007

Thesis Advisor:	David Brannan
Second Reader:	Michael Grossman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Bridging the Gap in Port Security; Network Centric Theory Applied to Public/Private Collaboration	**5. FUNDING NUMBERS**
6. AUTHOR(S) Candice L. Wright	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

"Achieving awareness in the maritime domain**,** including intelligence and information sharing at all levels of government is a key to our maritime security. Better awareness of what is out there leads to better unity of effort in maritime planning and operations. We need to have a common operating picture. We also need to integrate our operational capabilities and efforts with our private sector partners to better prepare for, respond to, and recover from incidents." –Admiral Thad Allen, 2007

The application of Network Centric Warfare theory enables all port stakeholders to better prepare for a disaster through increased information sharing and collaboration. Currently, a significant gap in connectivity exists among the many entities responsible for securing the intermodal supply chain throughout the port complex. The research conducted in this thesis creates an architecture using the theory of Network Centric Warfare to perpetuate a cycle of preparedness in a seaport, thus enhancing situational awareness for improved security. As a result of the research conducted in this thesis, the architecture is being applied in the Port of Los Angeles/ Long Beach in the form of a public/private "virtual maritime fusion center" to fill the gap between stakeholders thus improving overall maritime domain awareness.

14. SUBJECT TERMS Maritime Security, Port Security, Network Centric Operations, Public/Private Collaboration	**15. NUMBER OF PAGES** 81
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

BRIDGING THE GAP IN PORT SECURITY; NETWORK CENTRIC THEORY APPLIED TO PUBLIC/PRIVATE COLLABORATION

Candice L. Wright
Detective, Long Beach Police Department
B.S., Chapman University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2007**

Author: Candice L. Wright

Approved by: David Brannan
Thesis Advisor

Michael Grossman
Second Reader

Professor Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

“Achieving awareness in the maritime domain, including intelligence and information sharing at all levels of government is a key to our maritime security. Better awareness of what is out there leads to better unity of effort in maritime planning and operations. We need to have a common operating picture. We also need to integrate our operational capabilities and efforts with our private sector partners to better prepare for, respond to, and recover from incidents.” –Admiral Thad Allen, 2007.

The application of Network Centric Warfare theory enables all port stakeholders to better prepare for a disaster through increased information sharing and collaboration. Currently, a significant gap in connectivity exists among the many entities responsible for securing the intermodal supply chain throughout the port complex. The research conducted in this thesis creates an architecture using the theory of Network Centric Warfare to perpetuate a cycle of preparedness in a seaport, thus enhancing situational awareness for improved security. As a result of the research conducted in this thesis, the architecture is being applied in the Port of Los Angeles/ Long Beach in the form of a public/private “virtual maritime fusion center” to fill the gap between stakeholders thus improving overall maritime domain awareness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AMSC	Area Maritime Security Committee
BSA	Battle Space Awareness
COP	Common Operational Picture
C-TPAT	Customs Trade Partnership Agreement Treaty
CSI	Container Security Initiative
DHS	Department of Homeland Security
DoD	Department of Defense
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICS	Incident Command System
JRIC	Joint Regional Intelligence Center
JTTF	Joint Terrorism Task Force
LA/LB	Los Angeles/Long Beach
MDA	Maritime Domain Awareness
NSMS	National Strategy for Maritime Security
NCW	Network-Centric Warfare
NY/NJ	New York/New Jersey
NSPD	National Security Presidential Directive
NIMS	National Incident Management System
NRP	National Response Plan
PPIC	Public Policy Institute of California
SOP	Standard Operating Procedure
TWIC	Transportation Worker Identification Credential
VPN	Virtual Private Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The Center for Homeland Defense and Security has been an amazing experience, and the knowledge I have gained here will be applied towards homeland security efforts for years to come. This thesis would not have been possible without the generous support of family, friends and colleagues.

Dr. Pelfrey, your confidence and kind words of encouragement resonated with me throughout the writing of this thesis. To the outstanding members of cohorts 0503/0504, thank you for the “30,000 foot view” and transference of great knowledge in this emergent field of Homeland Security.

Dave Brannan, your guidance and friendship throughout the CHDS program and unrelenting dedication during the writing of this thesis mean the world to me. Commander Mike Grossman, Los Angeles County Sheriff’s Department, your knowledge, experience and encouragement helped immeasurably in completing this thesis, and for that I am grateful.

Sgt. Erik Herzog, Long Beach Police Department, your patience, advice and confidence in me, be it on a daily basis or during this endeavor, is invaluable.

To my parents and great friend Marta, I am indebted to you for all your efforts in keeping my family afloat when I was away.

Will, your love and humor made this arduous process obtainable, and I appreciate the support when I needed it most. Finally, to my children Noah and Keeley, you are my strength and true inspiration. I love you both “to infinity and beyond.”

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In 2004, National Security Presidential Directive (NSPD) 41/Homeland Security Presidential Directive (HSPD) 13 outlined the need for a National Maritime Security Policy. The National Maritime Security Strategy was completed along with eight supporting plans. These plans establish a comprehensive Maritime Domain Awareness (MDA) plan including preventive guidelines for securing the waterways from a terrorist attack and the joint efforts to respond to one. Each maritime plan stresses the inclusion of the private sector and the coordinated efforts which must occur in order to properly and thoroughly secure our nation's seaports.

On May 25, 2006, The Department of Homeland Security released the latest version of the National Response Plan (NRP). This plan establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The NRP forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents[1].

The NRP and the National Maritime Strategy both underpin the need for coordinated efforts across all sectors of government and industry to secure our nation. Even though the emphasis of collaboration is clearly the direction of most homeland security plans, very few successful public/private collaborative programs have been implemented on a large scale to include the maritime domain. In recent years several comprehensive assessments have specifically examined the complexities of port security. The Public Policy Institute of California (PPIC)[2] and Stevens Institute of Technology[3] cite complicated jurisdictional venues that inherently stove-pipe security as a primary obstacle to secure our nation's economic pulse point.

[1] U.S. Department of Homeland Security, www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf [Accessed January 21, 2007.

[2] Public Policy Institute of California.2006. *Protecting the Nation's Seaports: Balancing Security and Cost involving the Los Angeles/Long Beach Port Complex* (2006).

[3] *Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism (*Hoboken, NJ: Stevens Institute of Technology 2004).

For example, the Port of Los Angeles/Long Beach is a complex jurisdictional network that interfaces with more than fifteen different law enforcement agencies,[4] two separate cities with two mayors, five county supervisors, 10 harbor commissioners and 24 city council members. Each operates under a number of federal, state and local guidelines that assign management resources for emergencies to different agencies depending on the circumstances.[5] The attempt to integrate a multitude of private security companies tasked with protecting our nation's critical infrastructure adds to the complexity.

As the recognition of the significance of port security increases, so does the involvement of local, state and federal law enforcement agencies. The national push to establish collaborative efforts to secure the homeland is evident at all levels of government. The creation of a Critical Infrastructure/Port Joint Terrorism Task Force (JTTF) in the LA/LB Port Complex emphasizes securing critical infrastructures as well as economic interests. This JTTF is comprised of federal, state and local law enforcement agencies working together with the specific goal of preventing and investigating acts of terrorism committed against critical infrastructure in the maritime supply chain[6]. This team of investigators is stationed near the LA/LB port complex in the Long Beach Resident Area of the Federal Bureau of Investigation.

Collaboration among the various law enforcement agencies in the greater Los Angeles Area has improved significantly to include a Joint Regional Intelligence Center (JRIC). Their purpose includes forming a collaborative bond to improve our nation's homeland security through the fusion of intelligence from multiple source reporting.

One evident gap in the port collaborative fabric is the incorporation of private stakeholders as a partner in securing the homeland and critical infrastructure, particularly in the areas of prevention, response and recovery. For example, in the port of LA/LB, there is no networked system currently in place wherein private security can (1) access

[4] The following entities have overlapping jurisdiction or collateral functions in the Port Complex: Long Beach and Los Angeles Police Departments, Long Beach Harbor Department, LA Port Police, Immigration and Customs Enforcement, FBI, Los Angeles County Sheriffs, Department of Homeland Security, CIA DEA and CHP.

[5] Public Policy Institute of California.2006. Protecting the Nation's Seaports: Balancing Security and Cost involving the Los Angeles/Long Beach Port Complex.

[6] Collateral duties of this squad include rail, air and domestic terrorism investigations.

intelligence bulletins, (2) report suspicious activity, (3) receive training and (4) immediately access situational reports during a live incident. Access to this information in a networked framework would give the private stakeholders, the true first responders a common operating picture in which to better secure the nation's vital infrastructure.

B. RESEARCH QUESTION

How can Network Centric Warfare theory be applied to public/private collaboration in an effort to increase overall maritime preparedness and security? Moreover, how would this theory support effective collection, dissemination of intelligence, sharing of information and situational awareness updates to portray a common operating picture in support of MDA?

C. SPECIFIC RESEARCH OBJECTIVES

The objective of this research reviews current maritime strategies and recommendations and applies a theory that supports four pillars of National Preparedness as listed in Homeland Security Presidential Directive (HSPD) 8: prevention, protection, response and recovery. This theory enables both public and private port stakeholders to better prepare for a disaster through increased information sharing and collaboration. Currently, a significant gap in connectivity exists among all the many entities responsible for homeland security in the port complex. The research conducted in this thesis creates an architecture using the theory of Network Centric Warfare (NCW)[7] to perpetuate The Cycle of Preparedness[8] in a port complex, thus enhancing situational awareness for improved security. The successful design and application as described herein could be a national and regional architecture linking federal, state, local and private industry with responsibility, authority or stake in matters of maritime security.

[7] Military theory allowing a common operating picture through information dissemination.

[8] William V. Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," *Journal of Homeland Security and Emergency Management* 2, no.1 (2005), http://www.bepress.com/jhsem/vol2/iss1/5 [Accessed May 20, 2006].

D. SIGNIFICANCE OF RESEARCH

Ports represent vital components to our economic well-being and are of major interest to our national security. In 2004, U.S. ports were responsible for $948 billion in waterborne trade and the future growth is predicted to only increase in the next 20 years. Moreover, ports provide major employment opportunities to more than 4 million people generating over $44 billion in annual income.

America's ports are also used as military platforms to protect our country as well as a logistical support base for Operation Enduring Freedom[9] and Operation Iraqi Freedom.[10] The terrorist threat to the Maritime Domain is real and potentially devastating as evidenced by past maritime attacks around the world. On October 12, 2000, al-Qaeda bombed the USS Cole in Yemen, resulting in 17 deaths and 39 injuries of U.S. sailors.[11] On December 25, 1993, The Palestine National Liberation Movement bombed an Israeli ship while it was docked in the port of Eilat resulting in 11 injuries.[12]

Any attack on the global maritime supply chain committed either in the United States or abroad would be devastating and the aftermath of destruction would be exacerbated if an attack were to occur in a major port such as LA/LB or NY/NJ. It is incumbent upon all key players, both public and private, to make a concerted, collaborative effort to secure our critical infrastructure. The research conducted within this thesis enhances MDA by providing a means to establish the private stakeholders as a full partner in the aspects of a disaster from prevention to recovery.

E. REVIEW OF RELEVANT LITERATURE

1. Maritime Security Strategies

a. National Strategy for Maritime Security

According to the strategy, "MDA requires information ranging from the detailed mapping of the coastal ocean floor to strategies that identify the multitude of

[9] Military operations in Afghanistan.

[10] Military operations in Iraq.

[11] MIPT http://www.tkb.org/Incident.jsp?incID=16298. [Last accessed January 12, 2007].

[12] Ibid.

vessels that operate along the more than 95,000 miles of shoreline and in the 25,000 miles of navigable waterways and 3.4 million square miles of open water that comprise the U.S. economic exclusion zone. MDA represents an important tool that can be employed to further protect the safety and security of the United States and the continued operation of the maritime transportation industry in U.S. waters."[13]

> In an effort to recognize and reduce vulnerabilities of U.S. ports and waterways following the attacks of September 11th, the United States Coast Guard has spearheaded an interagency approach for establishing MDA. The core of MDA efforts revolve around the development and use of accurate information, intelligence, and knowledge of vessels, cargo, crews, and passengers, and extend this well beyond traditional maritime boundaries. MDA is designed to provide a layered defense through collaborative efforts with international partners to identify and counter security risks long before they reach a U.S. port.[14]

NSPD 41/HSPD 13 defines "Maritime Domain" as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances.[15]

The National Strategy for Maritime Security states, "Maritime security is best achieved by blending public and private maritime security activities on a global scale into an integrated effort that addresses all maritime threats."[16] Although several efforts have been made to involve the private sector into homeland security, many of them are either voluntary or implemented by regulatory requirements. The leap to *integrating* (emphasis mine) private stakeholders with public entities has not yet been accomplished.

[13] The National Strategy for Maritime Security, Washington D.C. September, 2005.

[14] Ibid.

[15] National Security Presidential Directive (NSPD) 41 and Homeland Security Presidential Directive (HSPD) 13, December 2004.

[16] The National Strategy for Maritime Security, ii.

According to the strategy, a four-layered approach to maritime security must address vulnerabilities such as transportation, staff, passengers, conveyances, access control, cargo and baggage and ports and security en route to the US.[17] The four layers are described as:[18]

Physical protection is a fundamental layer including protected zones, access controls and barriers, fences, guards and surveillance equipment along with standards and procedures establishing minimum requirements for securing critical infrastructures.

Physical cargo inspections provide another layer of security wherein all inbound cargo is screened for WMD components. It also includes the establishment of mandatory reporting requirements provided by the private sector. All inbound cargo designated as high risk is preferably screened prior to loading.

Interdiction of personnel and materials that could pose a threat for the maritime domain is another essential layer of security. The interdiction applies to terrorist personnel, financing, WMD or other contraband as detected by coordinated intelligence and/or allocation of resources. It includes the monitoring of high interest vessel traffic and the movement of people and cargo from the point of origin to entry into the country. Inspections will be conducted when deemed appropriate.

Military and law enforcement response is the fourth layer of security. The strategy calls for a "well trained, properly equipped and ready maritime security force from both the U.S. Armed Forces and national, regional, state and local law enforcement agencies to detect, deter, interdict and defeat any potential adversary."[19]

The success of the National Maritime Strategy depends upon integrating public/private security efforts through the shared use of intelligence, resources, communication and *shared* situational awareness.

[17] The National Strategy for Maritime Security, 20.

[18] Ibid., 21

[19] Ibid., 22

The National Strategy for Maritime Security (NSMS) includes the following eight supporting implementation plans:

1. The National Plan to Achieve Maritime Domain Awareness
2. The Global Maritime Intelligence Integration Plan
3. The Maritime Operational Threat Response Plan
4. The International Outreach and Coordination Strategy
5. Maritime Infrastructure Recovery Plan
6. Maritime Transportation System Security Plan
7. Maritime Commerce Security Plan
8. The Domestic Outreach Plan

The aforementioned plans work in concert to enhance MDA for a more effective approach to homeland security and defense of the United States of America. While each of these plans are written by the federal government, the applicability stretches across jurisdictional boundaries from private maritime stakeholders to local, state and federal partners.

The foundational crux of many of these plans establishes the means by which to better share information and communicate more effectively among the entities responsible for enhancing MDA and overall preparedness and emergency response capabilities.

2. Network Theories and Frameworks

Outlining the military theory Network Centric Warfare—showing its applicability to the civilian realm and the Cycle of Preparedness are paramount in understanding how the two can compliment each other to assist in MDA and overall port security efforts. Chapter four will detail the theory and framework to provide background information to establish a foundation on which to proceed. Chapter five applies the theory and model to the maritime complex, describing how using each of the principles will address a particular port security need and/or process thus perpetuating the Cycle of Preparedness.

a. Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats

In the "Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," William V. Pelfrey identifies the need for governmental and non-governmental entities to follow a strategic framework for agencies to prepare in stages.[20] According to Pelfrey, simply arguing the fact of preparedness "…is hollow without a framework." Similarly, to argue that we are unprepared without clearly specifying how preparedness can be attained is insufficient to accomplishing the goal of preparedness."[21]

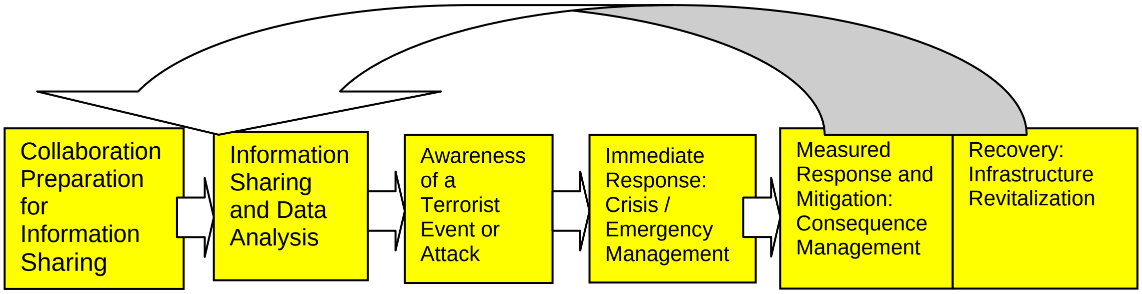

Collaboration Preparation for Information Sharing
Information Sharing and Data Analysis
Awareness of a Terrorist Event or Attack
Immediate Response: Crisis / Emergency Management
Measured Response and Mitigation: Consequence Management
Recovery: Infrastructure Revitalization

Figure 1. Major Elements of the Cycle of Preparedness

Several plans, including the National Response Plan (NRP) and the National Incident Management System (NIMS),[22] establish processes to implement national level plans in preparing for disasters. However, theses plans operate in a linear manner and progress through prevention, preparedness, response and finally recovery; usually referred to during and after an attack. "The Cycle" focuses on preparedness as a whole and uses collaboration and information sharing as a means to facilitate the four phases to preparedness. According to Pelfrey, these elements include; *Prevention, Awareness, Response and Recovery.*[23]

b. Network Centric Warfare Theory

The term "Network-Centric Warfare" (NCW) is a military term used to describe a common overarching theory to obtain and link various forms of intelligence,

[20] Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats" 6.

[21] Ibid., 1

[22] U.S. Department of Homeland Security, *National Incident Management System,* (March 1, 2004), U.S. Department for Homeland Security, *National Response Plan* , (December, 2004): 2-4.

[23] Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," 7.

process it and distribute it back out to the battle zone for dominant Battle Space Awareness (BSA) or common operating picture. BSA is defined by the Department of Defense as,", "The knowledge and understanding of the operational area's environment, factors, and conditions, including the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive and accurate assessments, in order to successfully apply combat power, protect the force and/or complete the mission." [24] The term "Network-Centric Operations" (NCO) is the process of implementing NCW.

NCW contains four basic tenets:

1) A robustly networked force improves information sharing.

2) Information sharing increases the quality of information and shared situational awareness.

3) This quality information and shared situational awareness enables collaboration and self-synchronization, while enhancing sustainability and speed of command.

4) These upgrades, in turn, provide the mechanism of advantage for increased mission capabilities.

The above tenets are supported by the following nine governing principles:[25]

1) Information Superiority

2) Shared Awareness

3) Speed of Command

4) Self-synchronization

5) Dispersed forces

6) Demassification

[24] Director, Force Transformation, Office of the Secretary of Defense. *The Implementation of Network-Centric Warfare*. (Washington DC: Office of the Secretary of Defense, January 5, 2005), 3.

[25] Ibid., 8.

7) Deep Sensor Reach

8) Alter Initial Conditions

9) Compressed Operations

These principles provide direction for operations in the Information Age. Both NCW tenets and principles are discussed at length in Chapter IV.

Both NCW theory and the Cycle of Preparedness can be applied to effectuate a higher level of MDA by including the private sector for a common operating picture and thereby improving port security. Utilizing the theory (NCW) to achieve and sustain the framework (The Cycle) creates basis from which to perpetuate networked collaboration and information sharing to facilitate preparation for preventing, protecting, responding and recovering from any disaster, natural or manmade in a port complex.

F. METHODOLOGY

The *Cycle of Preparedness*[26] framework, integrated with the tenets of Network Centric Operations, forms an architectural framework on which a solid regional collaborative program could be designed to embrace the private sector as a partner in port security. Dr. Pelfrey's model, supported by the tenets and principles of network centric warfare, is used as a template based on the four phases of prevention, preparedness, response and recovery. It also reviews existing programs used to facilitate public/private collaboration. Both theories are proven and accepted as independent models[27] used within the United States military as well as within Homeland Security models and frameworks.

1. Interview and Survey Method

The interview and survey method was used to assess the needs of port stakeholders and to determine where gaps presently exist the collaboration process. The interviews and surveys reached out to multiple stakeholders, all of whom have a portion

[26] Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats."

[27] The models have not been previously integrated and applied to port security.

of responsibility for securing critical infrastructure in the LA/LB Port Complex. The stakeholders include the Long Beach Police and Harbor Departments, the Los Angeles Port Police, The U.S. Coast Guard and The Los Angeles Police and Sheriffs Department. Facility security officers (FSO's) in the private sector such as American Presidential Lines, Long Beach Container Terminal, Maersk, Hanjin, SSA Marine Terminals and several representatives from the oil industry such as British Petroleum, Shell and Amerigas refineries also participated.

2. Case Study

a. Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign against Terrorism

This thesis also utilizes the case study method to examine the Stevens Institute Net-Centric analysis which was applied to the New York/New Jersey Port.[28] The structure, conception, sustainability and measurable results are examined as to its suitability and applicability in a national framework.

This report is especially relevant to this thesis due to its insightful analysis of the maritime industry as it encompasses a port complex (New York/New Jersey) with similar goals and attention paid to the private stakeholders. The outcome of this report outlines maritime threats, assessments, and network architectures, standardization of risk assessments, information architectures and Network centric approaches.

The Stevens Institute of Technology conducted a security analysis of the Port of New York/New Jersey and applied the concept of network centric operations.[29] The theory, as explained in the case of the NY/NJ Port, utilizes a net-centric approach to close the gaps in homeland security, particularly in jurisdictionally-challenged locations. The operative goal in this concept leverages new technology to integrate prevention, response and recovery through constant collaboration among *all* port stakeholders.

The study outlines an immediate need for a national and regional architecture that links federal, state, local and city organization that have the

[28] This concept has been used throughout the military.

[29] *Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism* (Hoboken: Stevens Institute of Technology, 2004).

responsibility, authority or stake in matters of homeland security. This architecture, as described by Stevens Institute,[30] provides a means to facilitate sharing of information across the key public and private organizations operating in the port region, plus a system to test, evaluate and train.

Second, the architecture should serve as a library or collection point for assembling and categorizing the many and diverse port security programs, projects and other initiatives currently underway. No such single collection agency exists, handicapping the ability to coordinate and exchange vital information and knowledge.

Third, a crucial part of the implementation process focuses on human factors, especially in the area of preparing for complex emergencies and becoming more reactive and efficient during events.

Fourth, the architecture can construct an electronic and cyber backbone linking the many agencies. The backbone must be secure, redundant, reliable, accessible and affordable. It must also possess sufficient redundancy to prevent and close communications gaps.

Stevens Study uses the Network Centric Theory and applies it to the port environment from the strategic level and then based upon the findings, develops a set of recommendations to be implemented in a test bed. This thesis examines the nine governing principles supporting Network Centric Operations, and then assesses and applies them to port security vulnerabilities to strengthen overall maritime security. Furthermore, the overall recommendations made by the report will be reviewed as well as a process by which these recommendations are being implemented in a pilot program in the Los Angeles/ Long Beach Port Complex .

[30] *Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism* (Hoboken: Stevens Institute of Technology, 2004) p.44

II. MARITIME COMPLEXITIES AND PROGRAMS

A. MARITIME COMPLEXITIES

Stakeholders in The United States currently operate 361 ports dispersed throughout the country, each having unique needs and challenges yet linked by waterborne trade. Each port operates a bit differently depending on the type and function of the port and level of intermodality. Some are major hubs of container distribution, some are major military staging points and still others are responsible for the nation's oil supply. However, one major commonality is the inherent vulnerability of each. Compounding the problem, many ports are located near major metropolitan areas, employ a large workforce and are geographically difficult to secure.

In 2005, The Journal of Homeland Security and Emergency Management released *U.S. Port Security Policy after 9/11: Overview and Evaluation.*[31] The following explanations of maritime/port complexities are contained within this report:

(1) Volume: An enormous amount of goods flow through the maritime supply chain. In 2004 alone, America handled almost 20 million ocean containers. This number has certainly risen in 2005 and growth is expected to continue to rise throughout the next twenty years.

(2) Intermodality: As ships enter the port the cargo is met with both rail and truck to disperse goods as quickly and efficiently as possible.

(3) Jurisdictional issues: The jurisdictional issues as noted earlier are intricate and potentially difficult as federal, state, local and private entities all have a piece of responsibility for security.

(4) Quantity of stakeholders: Carriers, shipping lines, labor unions, trucking companies, vessel tracking and pilot companies should be working together to secure commerce.

[31] Jon D. Havemen, Howard J.Shatz and Ernesto Vilchis. "Protecting the Nation's Seaports: Balancing Security and Cost," *Journal of Homeland Security and Emergency Management*2, no. 4 2005, article 1 (2005), www.bepress.com [Accessed January 1, 2007] 4.

(5) Global nature of business: The nature of the shipping industry is global; therefore, any comprehensive approach to port security must involve foreign partners.

(6) Time sensitivity: Every delay of commerce is money lost and services denied. Manufacturers rely on and plan for a steady stream of merchandise.

(7) Public and Private Interests: Sharing propriety information remains an issue. Each entity expects the other to finance security efforts. At times regulatory requirements impede the smooth and timely flow of commerce.

For example, the Los Angeles/Long Beach Port Complex is one of the most complicated maritime jurisdictions struggling to cohesively combine public/private efforts to enhance port security. The port operates amidst a metropolitan area of more than 10 million people with a labor force of almost 7.5 million and a median annual household income of $46,000. The twin ports account for 111 million tons of seaborne trade each year. It is the fifth-largest port complex in the world after Hong Kong, Singapore, Shanghai, and Shenzhen.[32]

The twin ports' combined import/export trade flow of $250 billion in 2004 is equivalent to about 30 percent of the greater Los Angeles gross regional product. Imports are five times larger than exports, and about half of the imports and two-thirds of the exports are to and from areas beyond the Los Angeles region.[33] This port is a strategic economic hub affecting the entire nation's economy.

Although the twin ports operate on a much larger scale than most, the jurisdictional complexities remain important in ports throughout the country. Multiple public and private entities, striving for security while balancing the flow of commerce, have no easy task, even in the most basic environments.

Post 9/11 saw the creation of an overall response framework with the advent of several security initiatives. The Maritime Transportation Security Act (MTSA) is included in this framework. The MTSA creates overall national, area, facility and vessel

[32] Jon D. Havemen, Howard J.Shatz and Ernesto Vilchis. "Protecting the Nation's Seaports: Balancing Security and Cost," *Journal of Homeland Security and Emergency Management*2, no. 4 2005, article 1 (2005), www.bepress.com [Accessed January 1, 2007] 73.

[33] Ibid., 75.

security plans; security response plans; the development of a worker identification card; rapid response boarding teams; vessel tracking systems; and the Area Maritime Security Committee (AMSC).[34] Several other programs such as The Customs Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI) and Operation Safe Commerce (OSC) have been created to facilitate both cooperative security measures as well as better regulate potentially harmful cargo in support of MDA.

B. MARITIME VOLUNTARY PROGRAMS

1. C-TPAT

> C-TPAT is beyond question, the largest and most successful government-private sector partnership to emerge from the ashes of 9/11
>
> - Robert C. Bonner

The C-TPAT program calls for business and government to work cohesively to secure and strengthen the supply chain. This program is voluntary and operates on a layered approach to securing cargo from port of debarkation to the port of call. The layers begin with security procedures, container security, physical access control, procedural security, security training and threat assessment, physical security, and information technology.[35]

2. Container Security Initiative (CSI)

In January 2002, Commissioner Bonner, head of U.S. Customs and Border Protection (CBP), announced the CSI program. CSI puts Customs officials in ports around the world to target high risk containers that may pose a terrorism risk.

[34] United States Coast Guard, *Area Maritime Security Committee Charter* (2004), http://www.uscg.mil/hq/g-m/mp/MTSA_Orientation/ams_overview.htm [Accessed January 1, 2007].

[35] United States Customs and Border Protection, http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_guideline/guideline_port.xml [Accessed January 2, 2007]

The four core elements of CSI include:[36]

- Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
- Prescreen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
- Use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma ray machines and radiation detection devices.
- Use smarter, more secure containers, which allows CBP officers at United States ports of arrival to identify containers that have been tampered with during transit.

3. Operation Safe Commerce (OSC)

Operation Safe Commerce is a pilot program designed to encourage deployment of technologies for ensuring containers' security as they move through the supply chain. A wide range of information technologies will be tested which include intrusion detection, container sealing and global positioning systems. The overall goal of OSC is to establish and determine best practices, policies and procedures for safe shipping that use technology to enhance security.

C-TPAT, CSI and OSC are intended to work in a cohesive environment with both the private sector and members from foreign governments. In port environments around the United States, several collaborative programs have been established in an attempt to open communication and intelligence dissemination to achieve better MDA. Although the following programs have been implemented, no method currently exists to link them.

[36] United States Customs and Border Protection, http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/security_guideline/guideline_port.xml [Accessed January 2, 2007].

Connecting them alleviates the inherent stovepipes that lead to failed collaborative efforts as decried by the National Maritime Strategy and several other Homeland Security Presidential Directives. Instead a robust network of networks would alleviate the "silos" we currently operate in and portray a common operating picture among all stakeholders.

C. MANDATORY PROGRAMS[37]

The following programs were written and implemented in response to increasing maritime security as part of the MTSA. These new regulations enable Customs officials as well as the Captain of the Port (COTP) to be aware of the specific vessels, commerce and crew entering U.S. Ports prior to the actual arrival of the ship.

- 96 hour Advance Notification of Arrival
- 24 hour Advance Cargo Manifest filing
- International Maritime Organization regulations
- Immigration and Naturalization Service Crewmember Security Plans

D. PUBLIC/PRIVATE PROGRAMS

1. InfraGard

One of the best known intelligence products geared towards the private sector is InfraGard. The Federal Bureau of Investigation (FBI) created InfraGard in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. In 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC). They have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal and security matters.[38]

[37] This is not all inclusive of the newly imposed security regulations, it is merely a sampling.

[38] Federal Bureau of Investigation Infragard www.infragard.net/about_us/facts.htm [Accessed December 30, 2006].

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.[39] The Los Angeles chapter of Infragard has developed a robust outreach initiative within the Maritime industry and has held several meetings in the Port of LA/LB.

The network of InfraGard is growing. It provides a useful tool for the FBI to reach out to the private sector.[40] The information and training available from the federal level remains a vital component to homeland security and should continue to be accessible to the private sector. This program should be considered and included in any overarching intelligence architecture.

2. Homeport

The United States Coast Guard has developed an information sharing program entitled Homeport. Federal Maritime Security Coordinators use Homeport as a primary means for the day-to-day management and communication of port security matters with Area Maritime Security Committee members, commercial vessel and facility owners and operators, government partners and the public. Homeport affords instant access to support increased information sharing requirements amongst federal, state, local and industry decision makers for security management and increased maritime domain awareness.[41]

Homeport is a publicly accessible internet portal providing all users with current maritime security information. It also serves as the Coast Guard's communication tool

[39] Federal Bureau of Investigation Infragard www.infragard.net/about_us/facts.htm [Accessed December 30, 2006].

[40] This program is a one way communication system

[41] United States Coast Guard, http://www.uscg.mil/hq/g-m/mp/pdf/final33cfr103.pdf [Accessed January 10, 2007].

designed to support the sharing, collection and dissemination of sensitive but unclassified information to targeted groups of registered users within the port community. As with InfraGard, Homeport is a vital tool in use by the Coast Guard, and it should be included in a larger networked architecture.

3. Area Maritime Security Committee

One of the mandates established by the MTSA was the designation of each Captain of the Port (COTP) as the Federal Maritime Security Coordinator (FMSC). The FMSC appoints an Area Maritime Security Committee (AMSC) to coordinate with industry partners to develop a comprehensive plan to further port security.[42] For example, the LA/LB COTP is the head of the Central California Area Maritime Security Committee (CCAMSC). They have defined the sector's mission as: Identify potential threats, improve security measures and procedures, improve communications, decrease vulnerabilities, coordinate contingency planning and conduct exercises.

Currently, the CCAMSC meets quarterly and is comprised of local, county, state, federal and industry representatives. The major accomplishments as noted by previous COTP Peter Neffenger[43] include the creation and publication of the first ever AMS Plan for Port Hueneme and the Ports of Los Angeles–Long Beach; improved response protocols; increased interagency operability; enhanced interagency communications; facilitated joint agency operations during heightened security alerts; and coordinated Incident Command Structure (ICS) training for maritime stakeholders.[44]

4. Joint Terrorism Task Force Critical Infrastructure Squad

During 1980, the Federal Bureau of Investigation (FBI) created the first JTTF in New York in response to an overwhelming number of bank robberies that were occurring in the city. The concept of the task force was successful and was soon applied to counter

[42] United States Coast Guard, http://www.uscg.mil/hq/g-m/mp/pdf/final33cfr103.pdf [Accessed January 10, 2007].

[43] Captain Neffenger was reassigned to USCG Headquarters in Washington D.C.. The current COTP is Paul Weidenhoft.

[44] United States Coast Guard, www.uscg.mil/d11/sectorlalb/documents/AMS101.ppt - 2006-01-24 [Accessed January 10, 2007].

terrorism measures. The current JTTF's primary responsibility is to respond to and investigate terrorist incidents or terrorist-related criminal activity. They proactively investigate domestic and foreign terrorist groups and individuals targeting or operating within the United States for the purpose of detecting, preventing and prosecuting their criminal activity. Theses collaborative investigative teams are currently housed in 100 cities nationwide, including at least one in each of the FBI's 56 field offices.45

Due to the increasing demands of securing our nation's critical infrastructure and the increasing emphasis placed on maritime security, the FBI created a new Critical Infrastructure JTTF. This squad's area of responsibility is the LA/LB port complex and includes critical infrastructures in and around the port such as oil refineries and rail lines. This "Port Squad" is comprised of local law enforcement agencies and federal agents assigned to this busy seaport. Established in October 2005, the squad resides in the Long Beach Residence Area of the Los Angeles Field Office of the FBI and works with industry partners as well as maintains the vice chair on the AMSC to foster a collaborative environment conducive to enhancing MDA.

As evidenced by the increase in port security grant funding, the guidelines within the MTSA and recently imposed security programs; the nation has made great strides in both increasing MDA and securing critical infrastructure. The added value of partnering with private industry is indisputable as displayed by the creation of Infragard, Homeport and the AMSC. Yet a gap still exists in connectively as these programs operate independently of each other. Currently, not one network links all of the agencies (public and private) with port security initiatives and collaborative programs.

To facilitate a common operating picture among all port stakeholders to enhance mission effectiveness (port security), a networked program should be established to link all of these valuable port security efforts together. Linked connectivity and cooperation among all stakeholders creates an environment wherein security efforts and disaster preparedness would grow within the private sector. Knowing that it is impossible to

[45] Federal Bureau of Investigation http://www.fbi.gov/page2/dec04/jttf120114.htm. [Last Accessed January 2, 2007].

prevent every attack by a determined terrorist, this connectivity also fosters and enables the flow of commerce. Port companies can conduct their business continuity plans, thus mitigating the effects of an attack.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SURVEY FINDINGS

A. INTRODUCTION

A regional survey was conducted in the LA/LB Port Complex and included federal state and local law enforcement as well as private facility security officers tasked with securing a variety of facilities in the port. The purpose of the survey determines the level of information sharing/collaboration within each sector independently as well as between the private sector and public sector. The survey was widely completed by representatives from all sectors, and it provides helpful insight on the issues at hand.

B. INSTRUMENT CONSTRUCTION

The Port Intelligence Survey was distributed to six intelligence subject matter experts from private, local, county, state and federal jurisdictions. Minor adjustments were made to the questions based on their expert feedback. The five point Likert forced choice[46] scale method was used in the construction of the survey. The four responses start with "strongly disagree" on one end to "strongly agree" on the other end.

The survey was prepared for "Zoomerang" online distribution and included 19 questions in 5 categories. The categories consisted of:

Collaboration

Intelligence sharing

Situational awareness

Training

Procedural information

The survey is designed with five questions investigating aspects of the collaboration category, four questions deal with the intelligence category and three ask

[46] Forced option scale eliminates the middle option of "neither agree nor disagree". This forces the participant to make a decision towards the affirmative or negative; removing neutrality.

situational awareness questions. Two are procedural questions, the training category asks three questions and two questions are designed to indicate employment.

The survey was distributed to 119 recipients, which comprises an accurate representation of the administrative, operational and strategic concerns of the port. Two respondents from the initial sample pool chose not to participate, one survey was undeliverable and, after further research, it was determined that six potential participants were no longer employed at the original and related assignments. Of the original 119 potential recipients, 51 fully completed the survey, and 5 partially completed the instrument. The respondents made a total of 67 visits to the survey site.   Of the participating sample pool, the respondents were divided fairly evenly with approximately 51% representing the private sector and 49% representing the public (law enforcement) sector.

C. SURVEY FINDINGS

The survey validates the research hypothesis. Serious gaps exist in the areas of communication, intelligence dissemination, training and standard operating procedures. A lack of situational awareness persists which prevents a common operating picture throughout the port. The most relevant data from the survey supporting the preceding statement was extracted and highlighted in the following five categories.

Collaboration

In the area of collaboration, 94% of respondents indicate they need more public/private collaboration to improve prevention, protection, response and recovery. Ninety-six percent think a networked system including intelligence dissemination, clear reporting procedures and situational updates would be useful in securing critical infrastructure. Only 43% are satisfied with public/private communication.

Intelligence

In the intelligence category, only 42%of the respondents were satisfied or very satisfied with the intelligence they received, and 46% percent thought the intelligence was actionable. Seventy-one percent of the private sector respondents report receiving intelligence bulletins on a seldom (monthly) or never basis, compared to 83.3% of their law enforcement counterparts, who report receiving intelligence products daily or weekly.

Situational Awareness

When respondents were asked how useful situational awareness (what is occurring throughout the port) would be for daily operations, 96% of the respondents reply useful or very useful. Conversely, only 30% report receiving updates on a daily or even weekly basis.

Training

In the area of disaster/terrorism training, 96% of the respondents agree more training would benefit their respective organizations. Only 36% report being satisfied with the amount of training they receive to secure critical infrastructure.

Procedures

Only 38% report that standard operating procedures exist between public/private stakeholders.

Miscellaneous Comments

The following comments are posted anonymously:

- "Too many agencies, no central point of contact or source of information in the port area."
- "More communication is needed at all levels. Information is sent to us; however, it is not in a timely manner. We usually have to solicit for information that is useful for us to operate efficiently during a crisis."

The data, as well as the additional comments, underscores the gap in collaboration between the public/private entities within the port complex. The following section displays the questions asked in the same format respondents accessed during the survey.

D. LIMITATIONS OF THE SURVEY

The sample pool was taken from researcher’s contacts, affiliates of the United States Coast Guard and Area Maritime Security Committee Members. The survey was distributed to 24 public law enforcement and 26 facility security officers. The participants were comprised of public and private entities from the LA/LB port complex and may or may not necessarily reflect the opinions of other ports across the country. This narrow pool sample represents one of the limitations of this survey and may reflect the biases of the geographical region. The research finds the results of the survey compatible with the research hypothesis, but it is not statistically binding. For further data included in the survey see appendix.

E. SUMMARY

Although many changes have occurred in homeland security since 9/11, the results of the survey underscore the need for a more structured and robust public/private collaboration. Both sectors recognize the need for more timely information and the benefits derived from that exchange. The road ahead utilizes technology to develop an architecture which facilitates the needs as described within the survey. The theory and framework to accomplish this arduous task are detailed throughout this thesis.

IV. NCW THEORY & THE "CYCLE"

A. NETWORK CENTRIC WARFARE THEORY

The term "Network Centric" originated in military operations and is gaining acceptance in the civilian world as well. "Network Centric Warfare" is the theory and "Network Centric Operations" is the implementation of the theory. "NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders intent."[47] NCW supports speed of command—the conversion of superior information position to action. NCW is transparent to mission, force size and geography. Furthermore, NCW has the potential to contribute to the coalescence of the tactical, operational and strategic levels of war. In brief, NCW is not narrowly about technology, but broadly about an emerging military response to the Information Age."[48]

Alberts, Garstka and Stein describe three key concepts of NCW, and they support both the theory and applicability of the theory. The first concept utilizes geographically dispersed forces and addresses the previous limitation of the military ability to: 1) communicate, 2) move and 3) project effects, forces needed to be collocated or in close proximity to the enemy or target they were defending. Due to these constraints, a geographically dispersed force is weak[49].

The second concept is a knowledgeable force obtained by steady information in a timely manner. By effectively utilizing the information gained, ground forces can evaluate the situation and make decisions quickly based on the totality of information. When applied to the battle space, a common operating picture enhances battle space knowledge.

[47] Commanders intent is defined as; A concise expression of the purpose of the operation and the desired end state.

[48] D.S. Alberts, J. J. Garstka, and F. P. Stein. "*Network Centric Warfare: Developing and Leveraging Information Superiority,*" CCRP Publications Distribution Center (1999), 15.

[49] Ibid., 90

Third, entities gain effective linking in the battle space. Effective linking requires the establishment of a robust, high performance information infrastructure or *info*structure that provides all elements of the warfighting enterprise with access to high-quality information services[50]

B. FOUR TENETS OF NCW

1. A robustly networked force improves information sharing.
2. Information sharing enhances the quality of information and shared situational awareness.
3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
4. These three improvements dramatically increase mission effectives.

C. NINE GOVERNING PRINCIPLES

According to the Department of Defense, Office of Force Transformation (DoD-OFT), [51] the following nine principles[52] support the tenets of NCW:

Information Superiority: Create information advantages through timeliness, accuracy and relevance. Increase enemy's information needs, reduce his ability to access information and raise his uncertainty; Assure our own information access through a well networked and interoperable force. Decrease our own information needs by exploiting our collectors.

Shared Awareness: Translate information and knowledge into common understanding and situational awareness for all participants. Build a network of networks, populated with quality intelligence and non-intelligence data to allow security

[50] D.S. Alberts, J. J. Garstka, and F. P. Stein. "*Network Centric Warfare: Developing and Leveraging Information Superiority,"* CCRP Publications Distribution Center (1999), 91- 92.

[51] Director, Force Transformation., 8.

[52] Although a military theory is being described; the principles have been written in this thesis as it applies to the civilian world and specifically port security.

forces to build shared awareness. Information users (private sector) must also become suppliers by posting information in a timely manner; Maintain secure networks and information that can be defended.

Speed of Command and Decision Making: Recognize information advantage and convert it to competitive advantage by developing process and procedures otherwise impossible. Through port security innovation and adaptation, make quicker decisions to turn information advantage into decision superiority and decisive effects. Block adversary's options and achieve enhanced security.

Self-Synchronization: Enable field level law enforcement and private security forces to operate almost autonomously and to redirect themselves through shared awareness and the commander's (leaders) intent. Increase the value of subordinate initiative to increase operational tempo and responsiveness. Assist in execution of commander's intent. Adapt to developing occurrences in the port complex.

Dispersed Forces: Move security forces from the traditionally deployed locations (stations/departments) to dispersed operations. Emphasize functional control versus physical occupation of the port and generate effective security power at the proper time and place. Increase intelligence, operations and logistics to achieve precise effects and gain global advantage with dispersed forces.

Demassification: Change from an approach based on geographically linked police and security forces to one based upon achieving effects. Use information to achieve desired effects without having to deploy mass physical forces within a specific geographical location. Increase tempo and speed of movement throughout the port complex to harden the critical infrastructure, complicating an opponent's target problem.

Deep Sensor Reach: Expand use of deployable, distributed and networked sensors,[53] both distant and proximate, that detect actionable information on items of interest at operationally relevant ranges to achieve decisive effects. Leverage increasingly persistent intelligence, surveillance and reconnaissance. Use sensors to gain

[53] Sensors include all entities that contribute to battle space awareness from satellites to "eyes on the ground."

and maintain information superiority. Exploit sensors as a deterrent when employed visibly as part of an overt display on intent. Enable every source to be a sensor, from the individual officer to a satellite.

After Initial Conditions: Exploit the principles of high-quality shared awareness, dynamic self-synchronization, dispersed and de-massed forces, deep sensor reach, compressed operations and levels of security, and rapid speed of command to enable the joint force to swiftly identify, adapt to and change an opponents operating context to our advantage. Historically, the close coupling in time of critical events have profoundly impacted the enemy, both psychologically (as a deterrent) and in locking out potential attacks.

Compressed Operations: Eliminate procedural boundaries between public/private collaboration entities within processes. Joint operations are conducted at the lowest organizational levels possible to achieve rapid and decisive effects. Increase collaboration in speed of deployment, employment and sustainment. Eliminate the compartmentalization of processes (e.g., organize, deploy, employ and sustain) and functional areas (e.g., operations, intelligence and logistics). Eliminate structural boundaries to merge capabilities at the lowest possible organizational levels, e.g. joint operations at the organizational/officer/security guard levels.

The following diagram[54] depicts the networking of the NCW principles through an informational, cognitive, social and physical domain. The informational knowledge allows the actors to move into awareness allowing for collaboration and the necessary application for mission effectiveness.

[54] Director, Force Transformation, 23.

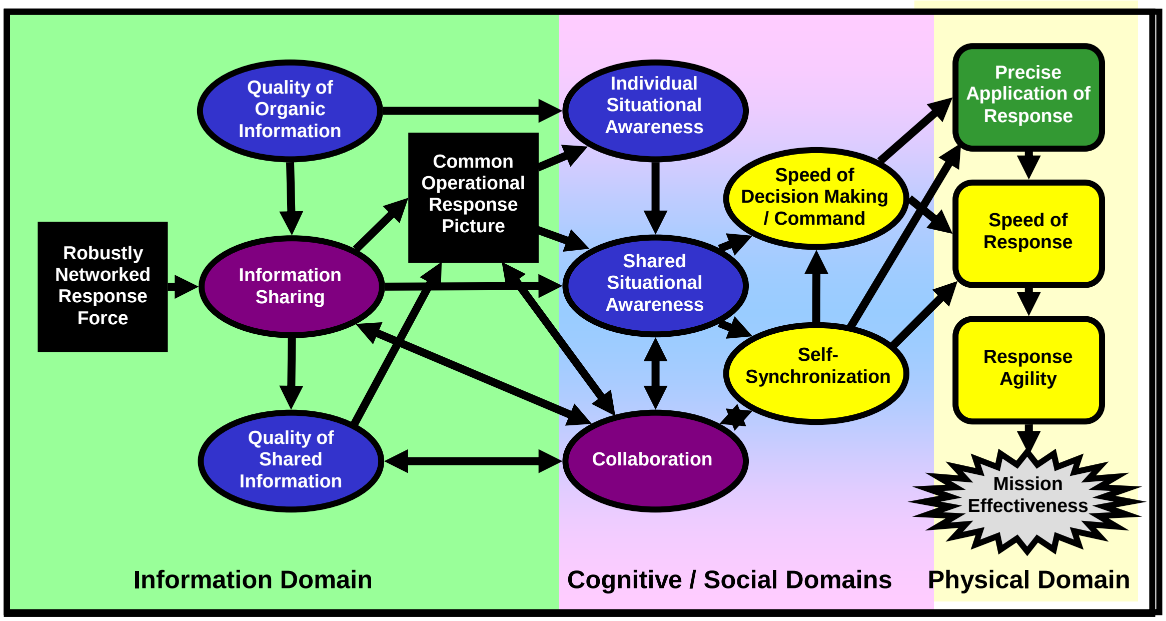

Quality of Organic Information
Individual Situational Awareness
Precise Application of Response
Common Operational Response Picture
Speed of Decision Making / Command
Speed of Response
Robustly Networked Response Force
Information Sharing
Shared Situational Awareness
Self-Synchronization
Response Agility
Quality of Shared Information
Collaboration
Mission Effectiveness
Information Domain
Cognitive / Social Domains
Physical Domain

Figure 2. Network Centric Theory

The Cycle of Preparedness

D. THE FRAMEWORK

Dr. Pelfrey describes a framework by which to accomplish an "auto adaptive" [55]capacity in organizations tasked with preventing, responding to and recovering from attacks. The framework starts with Prevention, accomplished through Collaboration and Information Sharing as primary elements. Threat Recognition, Risk Management and Intervention are additional elements, followed by Awareness that an event is occurring. The Response category is next, best characterized as emergency response activities. Consequence Management and Recovery to revitalize the jurisdictions is the final element in the cycle.[56]

The issue of preparedness is a primary goal of the Department of Homeland Security. Almost without exception, each new strategy, whether it is local, state or

[55] Louise Comfort, "Institutional Re-orientation and Change: Security as a Learning Strategy," The Forum 1, no. 2 (2002a): 1-5. Auto Adaptive is defined as "system of interacting units, each performing at its own rate but adjusting that performance to that of its near-neighbors in response to incoming information from the environment."

[56] The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats, William V. Pelfrey Journal of Homeland Security and Defense, Bepress 2005

federal, contains a component of preparation. However, as Pelfrey points out, the vision has not been clearly articulated or swiftly adopted. The following phases are parts of the cycle described individually, but together outline a framework to implement an overall preparedness strategy that is iterative, as opposed to the standard linear configuration of preparation.

E. THE FOUR PHASES

1. Prevention

Prevention is divided into five distinct elements: Collaboration, Information Sharing, Threat Recognition, Risk Management and Intervention. The two most important overarching elements to facilitate prevention is “Collaboration” and “Information sharing.”

Collaboration represents the most essential aspect of all. If organizations cannot work together, the other elements are incomplete and disjointed. Furthermore, collaboration includes collegiality, trust, flexibility, openness, mutual respect, social capital and pathways of communication.[57]

As collaboration is established, a pathway to information sharing increases frequency, validity and reliability of data. Information sharing, gathering and disseminating are crucial to prepare against acts of terrorism. Without it, any collaborative process will halt. Organizations must address two prerequisite elements: threat recognition and target hardening and intervention. If information sharing and collaboration are established, authorities can effectively identify threats, risks and vulnerabilities, properly harden targets and prevent an attack.

2. Awareness

The response process requires the knowledge or awareness that the event is occurring. This stage in the Cycle of Preparedness segues between pre-incident

[57] Pelfrey, “The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats,” 10.

prevention and post incident response.[58] The quicker organizations are aware of an incident regardless of the planning or operational stage, the better chance of stopping the incident from happening or at least mitigating its effects.

3. Response

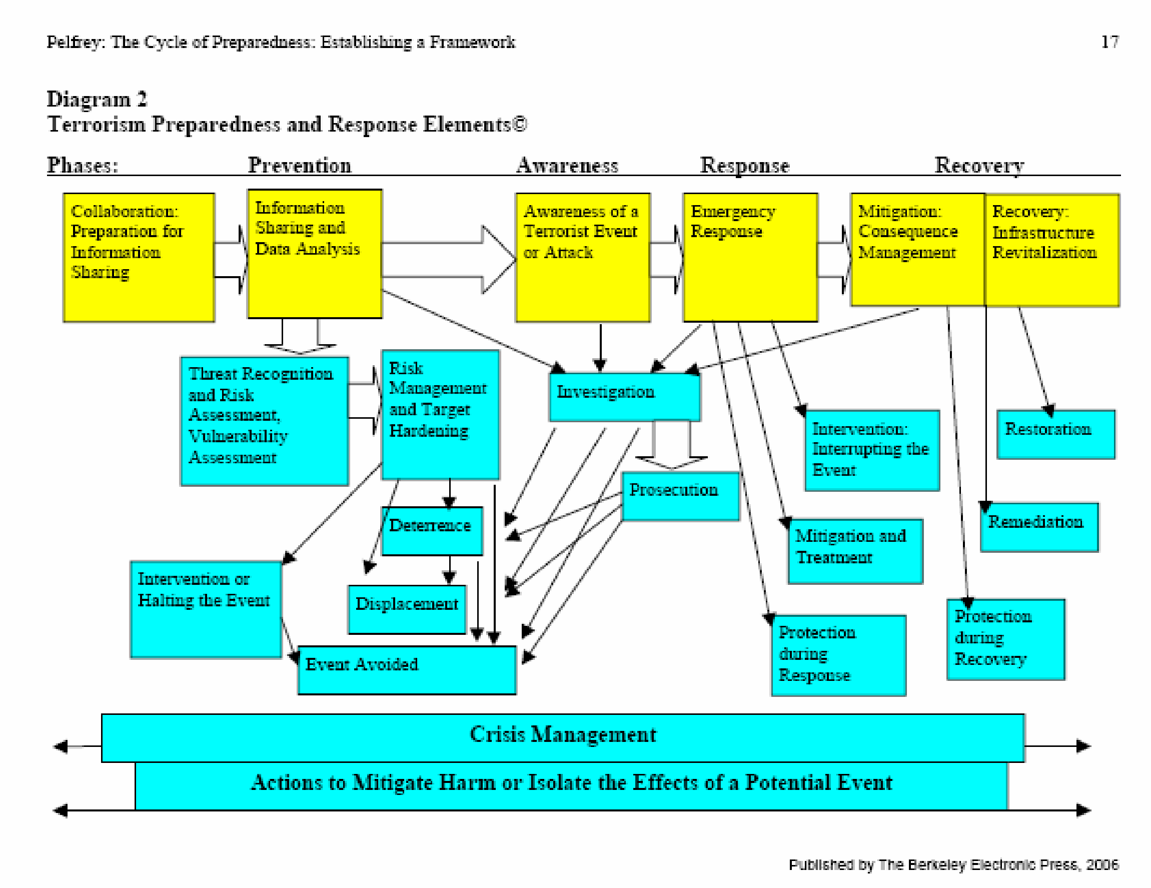
Response is the next category within preparedness and perhaps one of the most discussed and exercised. This phase relies on taking immediate action once a threat emerges. According to The Cycle, these actions include containment and control of a scene, incident management, mitigation, investigation and the preservation of life as a top priority.

4. Recovery

In accordance with the other three phases, it is crucial to prepare for recovery. The recovery process does not activate separate from response; it is not simply a linear process. Some organizations will be in the recovery process while others may still be actively responding. Nonetheless, the most effective and efficient way to prepare for recovery occurs through the use of good collaboration, planning and information sharing prior to and during an event. Pelfrey describes the following diagram as placing the elements in distinct phases to suggest a strategic model to integrate these elements and reflect a more complete version of the model.[59]

[58] Pelfrey, “The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats,” 10.

[59] Ibid., 3.



Pelfrey: The Cycle of Preparedness: Establishing a Framework 17

Diagram 2
Terrorism Preparedness and Response Elements©

Phases:
Prevention
Awareness
Response
Recovery
Collaboration: Preparation for Information Sharing
Information Sharing and Data Analysis
Awareness of a Terrorist Event or Attack
Emergency Response
Mitigation: Consequence Management
Recovery: Infrastructure Revitalization
Threat Recognition and Risk Assessment, Vulnerability Assessment
Risk Management and Target Hardening
Investigation
Intervention: Interrupting the Event
Restoration
Prosecution
Remediation
Deterrence
Mitigation and Treatment
Intervention or Halting the Event
Displacement
Protection during Recovery
Event Avoided
Protection during Response
Crisis Management
Actions to Mitigate Harm or Isolate the Effects of a Potential Event

Published by The Berkeley Electronic Press, 2006

Figure 3. Terrorism Preparedness and Response Elements

V. NCW AND “CYCLE” MARITIME APPLICATIONS

A. PRINCIPLES AND NCW APPLIED TO PORT ENVIRONMENT

Network Centric Theory is appropriate and useful in developing architecture to enhance MDA. It closes the gaps between the public and private sector which currently render port security less effective. The nine governing principles described in the preceding chapter are particularly relevant. Each component, when applied to a port security situation or gap, enhances overall security throughout the port complex. This chapter implements NCW concepts as it applies *operationally* in the port complex with an emphasis on networking with the private sector.

The progression from the Industrial age to the Information age changed many policies, procedures and ways of thinking. The world operates in a vastly different sphere, and the theaters of war and homeland security are no exceptions. The need for innovation and adaptation to confront today’s networked security threats birthed the NCW concept. Web technology is the foundational driver of that concept.

Utilizing a virtual private network (VPN) allows public/private stakeholders to collaborate in a networked environment. Once the VPN is installed and the stakeholders are connected, the technology creates a framework that applies the nine principles. The following is an example of applying those principles using information technology to gain MDA and includes the private sector.

Information Superiority

A well-networked force creates a network of networks.[60] For example, most of the private facilities in the port have sister companies throughout the world making the network global in nature. The ability to disseminate and collect information worldwide at the speed of a button greatly enhances information superiority.

Two-way information sharing allows the intelligence to be “pushed” down while at the same time allowing for information to be “pushed” up. This information may

[60] Network of networks refers to the linking of established networks with other established networks.

include requests for information on suspicious people, cargo or activity or the release of intelligence bulletins detailing the latest maritime threat information.

Shared Awareness

Several programs and intelligence databases[61] currently exist in an effort to facilitate a relationship with the private sector. Most of these programs operate independently, creating potential stovepipes of gathered intelligence. The networked system links these previously stove-piped systems and makes them easily accessible to both the public and private sectors in a central location. Once the information is in a common location, it is easily disseminated and/or retrieved throughout the port complex for shared situational awareness.

Dissemination of real time information represents another advantage of the network. This information could include threat, planning or routine operational information allowing for continuity of operations; appropriate response measures; or even evacuation information. As the survey indicates, shared awareness remains a vital component of port operations and is not currently in place

For example, in LA/LB two major suspension bridges[62] and one lift bridge[63] links both sides of the port and Terminal Island. Theses bridges not only serve as a link among the two cities, but they serve as the major ingress/egress routes for commerce entering and leaving the ports. If one of the bridges reported a bomb threat or suspicious device, law enforcement would halt commerce in the affected area until they resolved the situation. No mechanism currently exists to disseminate that information en masse, in real time to the industries so that they can re-route their commerce flow in line with business continuity plans, thus mitigating the effects of an attack or the mere threat of one. That significant lack of shared awareness is vital to the economic supply chain.

[61] As mentioned previously: Infragard, Homeport, Titan, DHS Bulletins

[62] Vincent Thomas and Gerald Thomas

[63] Schuyler Heim Bridge

Speed of Command and Decision Making

The requirements for speed of command as it relates to port security are two-fold. The first requirement educates the players to recognize suspicious activity and anomalies prior to an actual threat. The prior training theoretically enables instant threat recognition, and provides the means to report it throughout the complex in a timely manner. Second, law enforcement agencies and the private sectors must agree upon and implement standard operating procedures (SOPs) including reporting procedures. The combination of these two practices in the network enhances speed of command and decision making, hardening the target.

Without the establishment of this principle, facility security officers feel obliged (and are sometimes encouraged) to call a host of law enforcement agencies looking for the correct one to respond to the ensuing incident. This protocol creates frustration and hesitation to report seemingly innocuous events that when linked together could portray a more substantial threat. Businesses and government must make that link before rather than after an event to more effectively secure the domain.

Self-Synchronization

Training, exercising and establishing SOPs enable the private sector and field law enforcement units to operate virtually autonomously and execute commanders' intent to mitigate a threat or incident in progress. Situational reports perpetuate self-synchronization, and shared awareness allows security units to rapidly respond to developing and changing events.

Dispersed Forces/Demassification[64]

Many private stakeholders in the port complex have security systems and technologies unrivaled by most government entities, specifically their impressive surveillance systems. Leveraging the maritime industry's surveillance capabilities

[64] Demassification refers to effectively positioning security forces through information and other sensors

(without exploiting proprietary information) significantly increases a shared awareness, a common operating picture and the ability to place security personnel in the most vulnerable positions.

Robust surveillance systems enable ground forces to disperse throughout the port according to the current intelligence information. This manpower dispersal can redeploy quickly, utilizing speed of command and decision making.

The ability to use technologies and intelligence in the port to conduct ground operations by positioning a reduced number of physical forces and logistics represents an application of dispersed forces and demassification.

Deep Sensor Reach

Sensors include all things contributing to battle space (maritime domain) awareness, from satellites to "eyes on the ground" and every capability in between. As it applies to the civilian world, this definition includes surveillance technologies, all source intelligence collectors, tracking systems and human intelligence.

The maritime industry is rich with intelligence source and global access. The key is to network the "sensors" and leverage the information to maintain security awareness and superiority. In the maritime arena this network includes linked surveillance camera systems, satellite tracking capabilities, connectivity with the C-TPAT and CSI initiatives, all source intelligence collectors (DHS, FBI, JRIC e.g.) and/or disseminators and customers of that product.

After Initial Conditions/Compressed Operations

Many of the governing principles are interwoven in a nonlinear manner, even when applied to port security needs, reflecting the essence and strength of NCW. The establishment of networked systems and information flow and the emergence of an interlocking web appear to lessen the likelihood of a vital component slipping through.

A prime component of compressed operations is the elimination of procedural boundaries by establishing SOPs and memorandums of understanding (MOUs) among the participating sectors. Compressed operations allow entities to work together even at the lowest operational levels, facilitating an environment of conjoined forces.

B. NCW TRANSFORMS VULNERABILITIES INTO STRENGTHS

Chapter II examines the inherent maritime complexities and vulnerabilities through the U.S. Port Security Policy after 9/11: Overview and Evaluation. While the term "inherent" vulnerabilities in maritime security is applicable, NCW tenets can significantly harden and/or mitigate the weaknesses. In several cases, applying centric theory can transform the vulnerabilities and capitalize on them as strengths. The following section studies the listed vulnerabilities and 1) explains the process of mitigating the weakness and/or 2) illustrates the progression from vulnerability to networked superiority.

Volume and Time Sensitivity—Trade growth in the maritime environment and throughout inter-modal supply chain is expected to grow exponentially in the next twenty years. With that projection, security measures should not only include protective measures but strong response and recovery plans mitigating the effects of an attack. The Maritime Commerce Security Plan[65] states, "…(maritime supply chain security) will be achieved by creating a framework that will support the *identification* of threats as early as possible…improve the *information* available for risk management, invest in technology to identify threats, develop security requirements and work in *partnership* with industry and the international community to promote global supply chain security."[66]

Network Centric concepts enable the safer movement of large volumes of commerce in a timely manner by disseminating network information for Speed of Command and Decision Making. Quickly determining the threat level prior to loading allows for more efficient distribution of commerce and time sensitive materials.

[65] *Maritime Commerce Security Plan* (Washington D.C., October 2005): 5.

[66] Ibid., 5.

In the event of a disaster, networked concepts such as deep sensor reach, shared awareness, speed of command and decision-making significantly reduce the interruptions in the flow of commerce, mitigating effects to the supply chain regardless of volume.

Programs such as C-TPAT and CSI partner with industry to streamline the flow of commerce, keeping with the demands of time-sensitive goods. These programs encourage partners to strengthen security measures within their organizations and are rewarded with an expedited process through Customs.

Intermodality—The maritime transportation system provides the backbone of the intermodal supply chain, and it is a complex chain including shipping, trucking and rail components. The vulnerability lies within connecting all links in this supply chain for overall commerce security. The NCW principles applied in a networked system actually convert this weakness into a supply chain strength by garnering information from multiple sources (deep sensor reach) and disseminating that information throughout the chain, increasing speed of command and decision-making effectiveness.

Jurisdictional issues—The sheer number of law enforcement entities operating and affecting port operations is at times overwhelming. Without proper communication and conjoined efforts among law enforcement entities, inevitable stovepipes create a complex weakness. The successful attacks on 9/11 one of the major reasons the disaster was not stopped before it was initiated was The lack of communication among the intelligence community (vulnerability) enabled the successful attacks on 9/11 and prevented the disaster. However, by sharing information though a networked system, your intelligence and information source has widened significantly alleviating stovepipes (strength).

The greater law enforcement community (federal, state and local) realizes the benefits of collaboration as evidenced by the creation of the JRIC fusion center, JTTFs and the AMSC, specifically in the port environment. However, these efforts are not linked through a cyber backbone and do not include private entities. By conjoining public/private efforts in a transparent environment, each organization brings their respective resources and expertise into the network, turning this vulnerability into a strength. It makes it easier and more likely to prevent future attacks because law enforcement and other entities can transcend the traditional barriers to communication. The greatest attributed strength of NCW (although several others apply) is how Information Superiority and Shared Awareness become part of the day-to-day effectiveness rather than a continuing vulnerability.

Quantity of stakeholders—The sheer number of stakeholders in the port environment initially overwhelms. A vast number of different industries work side by side (yet autonomously) to ensure the most effective distribution of goods. Each organization is responsible for their respective piece of commerce flow and only come together when distribution requires it. This economically driven fact impedes greater security in the ports.

For example, in LA/LB Port Complex, some of the major private industries and organizations operating within the maritime arena (both on the water and shore side) include container terminals (shipping lines); dry bulk and break bulk terminals; oil refineries; dock workers (International Longshoreman's Warehouse Union); tug boat and pilot operators; pleasure craft marinas; and cruise ship terminals. The diverse nature of the stakeholders, coupled with the number of separate entities potentially involved in sharing information in the port, clearly overwhelms traditional liner methods of dissemination.

Communicating and collaborating with each of these disparate entities presents an arduous task which most certainly contributes to port security vulnerability. However, many of these industries have self-organized into longstanding associations (networks) for their respective industries. Leveraging the pre-established networks and creating a "network of networks" operating through the cyber backbone allows for transparency, connectivity and seamless information flow. When approached in a linear manner, that the network transforms the vulnerability to a strength. This disparate mass of stakeholders transforms into a thriving network displaying the governing principles[67] of NCW, in turn creating a common operating picture throughout the port and greatly enhancing MDA.

[67] Details of the principles can be found in Chapter Four.

Public and Private interests—A delicate balance exists between the privacy rights of the industries engaged in free trade within the port and the increased security need. This challenge has been debated throughout government. At times, the goals of the two seem contradictory. Regulatory requirements at times conflict with timely flow, creating vulnerability. Chapter Four outlines several of the governing principles of NCW that both allow and thrive on public/private collaboration, therefore extending and supporting the much needed cycle of preparedness.

Garnering the capabilities and expertise of each sector only strengthens the network. The obstacles such as regulatory issues and proprietary information can be overcome by establishing SOP's /MOU's that clearly delineate roles and responsibilities of each sector. The resources of private industry, including surveillance capabilities, specialty equipment and industry expertise, clearly play a role in strengthening prevention, response and recovery efforts.

The **Global nature** of the maritime domain encompasses trade routes, communications links and natural resources vital to the global economy and the well-being of people in the United States and around the world.[68] The application of network centric operation thrives in this environment. The strengths of the theory allow effective communication and operation through the established networks, regardless of geographic location. In fact, the larger the geographic area, the increased need for the application of the theory and greater effectiveness of the operation due to the increase in information flow from a greater numbers of sensors leading to a larger common operating picture.

The National Strategy for Maritime Security also addresses the need for global outreach and outlines it in the supporting plan entitled International Outreach and Coordination Strategy. This strategy addresses specific goals of increasing MDA with specific strategic objectives. The common thread throughout the plan coordinates and integrates maritime security across foreign, international and regional boundaries.

Applying the tenets and governing principles of NCW transforms the reported maritime vulnerabilities and leverages them as strengths within the supply chain. The

[68] *International Outreach and Coordination Strategy (*Washington D.C., November 2005) : 1.

establishment of this network also creates a solid public/private relationship that is reinforced through a robust network with a growth potential for future trends

C. NCW PERPETUATES “THE CYCLE” IN PORT SECURITY

The Cycle of Preparedness provides a framework by which to prepare for any disaster in the port complex. The process of preparedness as described in The Cycle contains multiple elements and phases. It does not operate in a linear manner, much like network centric operations. Pelfrey describes two predicate elements of the Cycle, collaboration and information–sharing, as “…enable[ing] agencies, jurisdictions, and organizations to effectively perform the other three elements of prevention, Threat Recognition, Target Hardening and Intervention.” These predicate elements reflect the very tenets that facilitate NCW and enable the governing principles to support it.

Other parallels emerge between the principles of network centric operation and the elements in the Cycle of Preparedness. The term “auto-adaptive” is referred to as a process in readiness for terrorist threats. Pelfrey describes the Cycle as “…a dynamic, flexible, and continuous process of interaction and integration, and functioning as a self-organizing mechanism that improves preparedness…”[69] Both of these descriptions are very similar to the “net-centricity” aspects of NCW and relate specifically to self-synchronization.

Pelfrey states, “A key objective of the Cycle of Preparedness is to establish processes and tools within the framework of the preparedness cycle and if it [the Cycle] is operationalized properly, it should represent a ‘systematic effort to create change in the performance of the whole system' as described by Louise Comfort.”[70]

Despite the many parallels among the theory and the framework maritime security can apply and perpetuate the Cycle framework through the application of network centric operations.

[69] Pelfrey, “The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats,” 3.

[70] Comfort, Louise. Institutional Re-orientation and Change: security as a learning Strategy. The Forum.2002a. Volume 1, Number 2.pgs. 1-5.

The following diagram displays the individual domains as described by Pelfrey, and the principles of NCW that facilitate the Cycle of Preparedness.

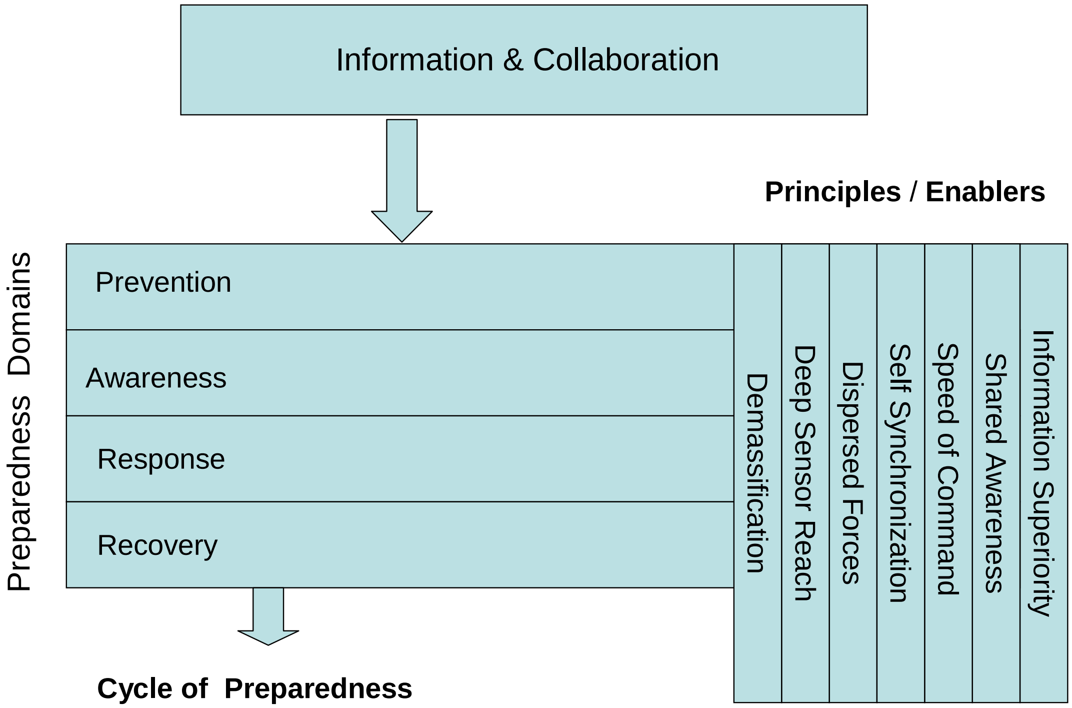


Figure 4. NCW and "Cycle"

VI. CONCLUSIONS

A. SUMMARY

"A strong world economy enhances our national security by advancing prosperity and freedom in the rest of the world. Economic growth supported by free trade and free markets creates new jobs and higher incomes."[71] The United States' role in the global economy is absolutely paramount. The main pillar of that role is the nation's position and influence on the economic supply chain. The vitality and integrity of that chain must be coveted and protected to the absolute best of our country's ability.

Over the last five years, congress has appropriated a total of $816 million for port security. The Coast Guard has stated that effective port security will cost $5.4 billion over ten years.[72] In January of 2007, the latest round of grant funding was announced. The Port Security Grant Program is being allocated $201.2 million dollars to increase port security measures across the country[73]. The monies invested by the federal government in the maritime industry have significantly increased in the past several years and testifies to the importance and emphasis of protecting and securing our economic vitality.

The strategic and operational goals to ensure economic security as well as physical protection of our country require a robust Maritime Domain Awareness. In the five years since the attacks on 9/11, our nation has undergone a significant change in the posture of our defense and security. The sanctuary we once lived and worked in has vanished, and we are no longer impervious to outside attacks which threaten the freedom on which this nation was built.

In an attempt to gain overarching MDA, the complexities and vulnerabilities in our country's seaports must be conjoined and strengthened to effectively meet the goals described and the need for adequate security. To see this goal to fruition, an environment

[71] The National Security Strategy of the United States of America. September, 2002.

[72] Robert Housman, "A Homeland Security Agenda for the First 100 Days of a Democratic-Led Congress," *Homeland Defense Journal* (December 2006): 48.

[73] PSGP Round 7 Announced, $201 Million for the Nation's Seaports, January 9, 2007 http://www.portsecuritynews.com [Accessed February 21, 2007].

of collaboration and cohesiveness among all of the stakeholders in the maritime arena must become second nature—the intellectual framework and specific execution issues which this thesis provide .

B. GAP IDENTIFICATION

This thesis identifies several gaps in port security that are hindering the true effectiveness of maritime security and the much-needed maritime domain awareness. The lack of a cyber linked network system linking all port stakeholders, even in a region such as LA/LB, represents a significant gap that needs to be reconciled. The establishment of a port JTTF is the FBI's attempt to foster a collaborative relationship among the law enforcement sector. It is a step in the right direction, but without the private sector, the picture is incomplete.

The private sector, particularly in the port environment, is essential in the facilitation of security throughout the complex. These organizations own and operate the majority of both water and landside operations conducted in the complex. Industries within the maritime arena are directly and significantly affected by the smallest of speed bumps occurring in that supply chain, let alone a major threat or worse, an attack. The delicate nature of the link between real or perceived dangers in the port by private sector stakeholders is both an economic and homeland security issue.

Including the private sector is not only mandatory, but it is imperative to the creation of a well-planned strategy and thorough security plan. Several programs have seen the value and capitalized on the expertise offered by private industries. FBI's Infragard[74] has been reaching out to companies through quarterly training and has a mechanism for disseminating information to them via email. The Coast Guard recently implemented Homeport[75] to reach out to civilian maritime partners. Although these initiatives provide positive examples of public/private programs, they do not fill the gap required to effectively implement port security. Much more must be done. Additional

[74] Federal Bureau of Investigation, www.infragard.org

[75] United States Coast Guard, www.Homeport.uscg.mil [Accessed March 10, 2007].

measures must meet the security needs and economic concerns of the private sector. They must follow a strategy that can be replicated in a manner that avoids further stovepipes of information or collaboration.

A vigorous public/private collaborative program requires architecture, including a cyber backbone, where information sharing paves the way for developing plans and protocols to support the four pillars[76] of the National Preparedness Goal (HSPD-8). This architecture's design allows port security participants to stop operating in a multitude of silos, ad hoc, without a single coordinating body. Furthermore, this design enables a framework to link all port stakeholders, to develop standard operating procedures and to present a common operating picture. Perhaps most importantly, the collaborative efforts described here meet not only the security and economic concerns of the stakeholders involved, but the cycles of preparedness continue and extend through the use of networks that appropriately address the asymmetrical nature of the threat.

The National Strategy for Maritime Security and the eight supporting plans[77] clearly call for and outline the need for extensive private sector involvement. Several entities are taking the steps to reach out into the community for involvement. Not linking these programs together though a network creates more modal stovepipes and further exacerbates this already complex venue.

C. THEORETICAL APPLICATIONS AND IMPLICATIONS

The Stevens Institute conducted an analysis of the application of Network Centric Operations in the Port of New York/New Jersey[78]. They also recommended a national or regional architecture to facilitate constant collaboration among all stakeholders.

By applying the principles of networking theory in the maritime environment, two clear issues surface. First, to effectively create overall maritime domain awareness, a framework for public/private collaboration must be designed and implemented. Once the

[76] The pillars are; prevention, protection, response and recovery.

[77] *The National Strategy for Maritime Security* (Washington D.C. September, 2005).

[78] Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism.

framework or architecture is in place, information flow through a well-networked force greatly enhances situational awareness and portrays a larger common operating picture. It subsequently fulfills the requirement of the National Preparedness Goal as directed by the President. Applying effective operational structures to national strategic security goals is an important benefit of following the course of action described in this thesis.

Second, and vastly more revealing, is the realization that when the theory is applied to the individual vulnerabilities, i.e. volume, intermodality, jurisdictional issues, quantity of stakeholders, global nature, time sensitivity and public/private interests[79], the vulnerabilities are transformed and leveraged as strengths within the supply chain**.**

After the vulnerabilities and complexities in port security are examined and a theory identified and applied to the issue, perpetuation of the Cycle of Preparedness achieves the end result. The Cycle of Preparedness is relevant because it implements HSPD-8 and fulfills the national direction and mandate of sharing information at "unprecedented levels." It is time to set theory aside and implement this notional solution at the operational level**.**

D. OPERATIONAL APPLICATIONS

The Los Angeles/Long Beach Port Applications of NCW

The applications outlined in the tenets and principles of NCW lay a theoretical framework and identify the areas benefited by proper placement of information. This foundation, when coupled with a cyber backbone, allows for a true public/private collaborative program.

Local law enforcement operating within the Los Angeles/Long Beach Port Complex are working in conjunction with private industry stakeholders to implement a public/private virtual maritime fusion center. The tenets and principles of NCW can be applied to increase overall port security. This program is based on the author's idea that disparate port related programs need to be linked for maximum effectiveness. This idea is subsequently validated by the research and findings in this thesis.

[79] Havemen, Shatz, and Vilchis, "Protecting the Nation's Seaports: Balancing Security and Cost."

The maritime fusion center utilizes a web-based virtual computer program that uses Microsoft Groove® software and features many collaborative tools such as discussion boards, stored picture capabilities, sketchpad options, live chat (two-way communication), e-mail and joint calendar tools. The fact that the software system being employed is built on architecture readily available to both government and the private sector is essential. In the event of a live situation, the programs can create ad hoc workspaces for operational planning and resources allocation coordination. This flexibility facilitates continued personal engagement, since those contacts take place within a structure that draws stakeholders in rather than excluding those that need the information most.

The maritime fusion center initially includes members of the Los Angeles and Long Beach Police Departments, and private industry heads responsible for aspects of maritime security from prevention through the stages to recovery. The program's ultimate goal networks the disparate entities (public and private) to facilitate a flow of information capable of supporting port-wide situational awareness and a common operating picture to enhance security and protect the nation's economic supply chain.

An interagency group has been appointed. They are responsible for writing a strategy outlining the goals and needs of the program, and guidelines and standard operating procedures ensuring a collaborative environment. This group is also responsible for setting goals and metrics to evaluate the program for utility and functionality, as well as vetting individuals granted access to the program to ensure its integrity. The inquiry is also confirming that consumers "know what they need to know" and producers understand exactly what intelligence and resources the consumers need to secure their infrastructure.

The working group in charge of designing the workspace realizes the uniqueness of the port environment and tailored the portal for the specific needs of its users. The functionality and utility of the network "office" requires the inclusion of the following areas or "rooms:"

Discussion Room—This area includes transparent discussions among law enforcement and private stakeholders on topics such as current threats, precautionary measures, area incidents, legislative or regulatory updates and any other related information.

Situational Awareness Room—Real time threats, law enforcement actions and/or current, live incidents that affect port operations[80]are posted in this area. This allows for facility security officers to self-synchronize by either evacuating their facility, enacting business continuity plans or remaining status quo if applicable. At a basic level, it gives the private sector the necessary information in a timely manner to properly secure his/her facility.

Reports and Guidelines Room—This area enables both law enforcement and private stakeholders to post current guidelines, standard operating procedures, regional requirements and even newly mandated programs. Again, this process allows for transparency throughout the port complex, alleviating silos and the lack of common procedures and polices.

Intelligence Bulletins Room—Unclassified intelligence bulletins are listed in this section from federal, open, military or private sector sources. This area's goal provides a single location to review intelligence applicable to the maritime and/or critical infrastructure sectors, preventing information overload.

Web-links Room—Several useful public/private online collaborations have been created and implemented such as Infragard and Homeport that issue useful and unique information. Through hyperlinks, users can access these programs from one central location. Other useful links are listed such as The Department of Homeland Security, Business Executives for National Security and the homepages of the United States Coast Guard, Los Angeles Police Department, Long Beach Police Department and the Federal Bureau of Investigations. Board members can approve adding websites upon per request.

Calendar Room—The calendar section organizes meetings, conferences and training events as they apply to MDA. Scheduling conflicts frequently arise among port

[80] This applies to operational information at the unclassified level.

entities hosting important, useful training and exercises. The calendar enables coordination among the port players so that primary information is not lost due to scheduling issues.

This thesis provides the intellectual and analytical framework for the operational design of a robust public/private collaborative network in a maritime environment. Additionally, this thesis outlines a program in the implementation phase which employs NCW theory and framework to bridge the collaborative gap currently seen in the region. The successful implementation of this program enables many of the components outlined in the National Strategy for Maritime Security and greatly enhances MDA by including the private sector. When it is operating at its fullest capacity and potential, the virtual maritime fusion center expects to apply the principles of network centric operations to perpetuate the Cycle of Preparedness and become a regional model for other ports to follow.

E. FURTHER RESEARCH

The ultimate goal of a fully robust networked architecture includes sensor data such as surveillance and tracking capabilities. With the expansion of technology, each port across the country can replicate this regional network. Once the respective ports establish the primary networks, each port network could link together to form a larger "network of networks." This string of networks supports the potential of creating global connectivity, a goal that extends both national and global security. The mini-networks linking international companies with the public sector all over the world facilitates this connectivity, creating a flow of information both vertically and horizontally and enhancing global maritime domain awareness.

The current LA/LB collaborative program uses technology which is reliable, secure, affordable and robust enough for the initial regional implementation. However, to achieve an overarching port intelligence network complete with sensor capabilities and global outreach, further research is needed to assess the technology currently available.

The breadth and depth of research needed to acquire the appropriate information technology software robust enough to fulfill the larger networking program requirements lies beyond the scope of this thesis.

LIST OF REFERENCES

Alberts, D. S., and J. J. Garstka. "Network Centric Operations Conceptual Framework Version 2.0." *U.S. Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration* (2004).

Alberts, D. S., J. J. Garstka, R. E. Hayes, and D. A. Signori. *Understanding Information Age Warfare*. Washington D.C.: DoD Command and Control Research, 2001.

Alberts, D. S., J. J. Garstka, and F. P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority." *CCRP Publications Distribution Center* (1999).

Cares, Jeff. *Distributed Networked Operations: The Foundations of Network Centric Warfare*. Rhode Island: Alidade Press, 2005.

Cleary, Christopher. "Strategy for Local Law Enforcement Agencies to Improve Collection, Analysis and Dissemination of Terrorist Information." Master's Thesis, Monterey, CA: Naval Postgraduate School, 2006.

Comfort, Louise. "Institutional Re-orientation and Change: Security as a Learning Strategy." *The Forum* 1, no. 2 (2002a): pp. 1-5.

Director, Force Transformation, Office of the Secretary of Defense. *The Implementation of Network-Centric Warfare*. Washington D.C.: Office of the Secretary of Defense, January 5, 2005.

Grossman, Michael. "Perception or Fact: Measuring The Effectiveness of the Terrorism Early Warning Group." Master's Thesis, Monterey, CA: Naval Postgraduate School, 2006.

Havemen, Jon D., Howard J. Shatz, and Ernesto Vilchis. Journal of Homeland Security and Emergency Management 2, no. 4, article 1 (2005) www.bepress.com [Accessed January 1, 2007].

Housman, Robert. "A Homeland Security Agenda for the First 100 Days of a Democratic-Led Congress." The Homeland Defense Journal (December 2006).

_____.Intelligence-Led Policing: The New Intelligence Architecture. Washington D.C.: Office of Justice Programs, United States Bureau of Justice Assistance, 2005.

International Association of Chiefs of Police. *From Hometown Security to Homeland Security*. Alexandria, VA: IACP, 2005. http://theiacp.org/leg_policy/HomelandSecurityWP.pdf [Accessed May 12, 2006].

International Association of Chiefs of Police. *Private Security/Public Policing Partnerships*. Alexandria, VA: IACP, 2004. http://www.cops.usdoj.gov/mime/open.pdf?Item=1355 [Accessed May 12, 2006].

______. *International Outreach and Coordination Strategy* (Washington D.C., November 2005).

Leary, T.P. "360 Port MDA-A Strategy To Improve Port Security." Master's Thesis. Monterey, CA: Naval Post Graduate School, September 2006.

______. *Maritime Commerce Security Plan* (Washington D.C., October 2005).

______. *Maritime Infrastructure Recovery Plan* (Washington D.C., April 2006).

National Security Presidential Directive NSPD-41 and Homeland Security Presidential Directive HSPD-13. *Maritime Security Policy* (December 21, 2004).

______. *The National Strategy for Maritime Security* (Washington D.C., September 2005).

New York State Office of Homeland Security. *Focus Report: Maritime Terrorist Threat* (February 2006). http://www.security.state.ny.us/training/national [Accessed November 16, 2007].

Office of Justice Programs. *Operation Cooperation Guidelines for Partnerships Between Law Enforcement & Private Security Organizations* (2000).

Pelfrey, William V. "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats." *Journal of Homeland Security and Emergency Management* 2, no. 1 (2005). http://www.bepress.com/jhsem/vol2/iss1/5 [Accessed May 20, 2006].

Police Executive Research Forum. *Protecting Your Community From Terrorism: Strategies for Local Law Enforcement* (November 2005). www.cops.usdoj.gov/Default.asp?Item=1361 [Accessed June 18, 2006].

______.*Private Security/Public Policing Partnerships* (2004). http://www.cops.usdoj.gov/mime/open.pdf?Item=1355 [Accessed May 12, 2006].

Public Policy Institute of California. *Protecting the Nation's Seaports: Balancing Security and Cost Involving the Los Angeles/Long Beach Port Complex* (2006).

Ronfeldt, D., and J. Arquilla. "Networks, Netwars The Future of Terror, Crime and Militancy." *RAND* (2001).

Securing the Port of New York and New Jersey: Network-Centric Operations Applied to the Campaign Against Terrorism. Hoboken, NJ: Stevens Institute of Technology, 2004.

———. *Terrorism Early Warning Group* (2005). http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf [Accessed June 3, 2006].

Tindall, James. "Applying Network Theory To Develop A Dedicated National Intelligence Network." Master's Thesis. Monterey, CA: Naval Postgraduate School, September 2006.

United States Coast Guard. *Area Maritime Security Committee Charter* (2004). http://www.uscg.mil/HQ/G-M/MP/pdf/AMSCSampleCharter1 [Accessed November 18, 2006].

U.S. Department of Homeland Security. *National Incident Management System.* Washington, D.C.: U.S. Department of Homeland Security, 2004.

U.S. Department of Homeland Security. *National Response Plan.* Washington, D.C.: U.S. Department of Homeland Security, 2004.

U.S. Department of Justice. *Engaging the Private Sector To Promote Homeland Security: Law Enforcement-Private Security Partnerships*. Washington DC: Office of Justice Programs, 2005. www.ojp.usdoj.gov [Accessed June 18, 2006].

Watts, R.B. "Implementing Maritime Domain Awareness." Master's Thesis. Monterey, CA: Naval Postgraduate School, March 2006.

Wilson, Clay. "Network Centric Warfare: Background and Oversight Issues for Congress." *CRS Report for Congress*, (March 18, 2005).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX

A. ZOOMERANG SURVEY RESULTS

1. More collaborative interaction between public/private stakeholders is needed to improve prevention, protection, response and recovery efforts.		
Strongly Disagree	0	0%
Disagree	3	6%
Agree	18	36%
Strongly Agree	29	58%
Total	50	100%

2. A networked system including intelligence dissemination, clear reporting procedures and situational updates would be useful in securing critical infrastructure.		
Strongly Disagree	0	0%
Disagree	2	4%
Agree	10	20%
Strongly Agree	38	76%
Total	50	100%

3. How often does your company participate in a collaborative meetings, training sessions or port exercises?		
Never	2	4%
Seldom (Monthly)	32	64%
Frequently (Weekly)	15	30%
Very Frequently (Daily)	1	2%
Total	50	100%

4. Do you currently participate in any networked system enhancing collaboration in the Port?		
No	24	48%
Yes	26	52%
Total	50	100%

5. Are you a member of any component of the Area Maritime Security Committee (AMSC)?		
No	20	40%
Yes	30	60%
Total	50	100%

6. Rate your level of SATISFACTION with the communication between the public and private stakeholders in the port.		
Very Dissatisfied	4	8%
Dissatisfied	24	49%
Satisfied	21	43%
Very Satisfied	0	0%
Total	49	100%

7. How useful would real time situational awareness be for your daily operations?		
Not Useful	1	2%
Useful	9	18%
Very Useful	39	78%
Unknown	1	2%
Total	50	100%

8. How often do you receive close to real time (within 10 minutes) situational updates during an incident occurring in the port?		
Never	8	16%
Seldom (Monthly)	27	54%
Frequently (Weekly)	11	22%
Very Frequently (Daily)	4	8%
Total	50	100%

9. How would you rate your level of satisfaction with the amount of intelligence information you receive?		
Very dissatisfied	3	6%
Dissatisfied	26	52%
Satisfied	20	40%
Very satisfied	1	2%
Total	50	100%

10. The intelligence bulletins I receive contain actionable information.		
Strongly Disagree	3	6%
Disagree	24	48%
Agree	23	46%
Strongly Agree	0	0%
Total	50	100%

11. How often do you receive intelligence briefs?		
Never	6	12%
Seldom (Monthly)	18	36%
Frequently (Weekly)	15	30%
Very Frequently (Daily)	11	22%
Total	50	100%

12. Approximate the percent of all intelligence bulletins you currently receive from each source.

Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option.	**0%**	**25%**	**50%**
Municipal Agencies __%	18	12	10
	44%	29%	24%
County Agencies __%	19	14	5
	48%	35%	12%
State Agencies __%	19	16	0
	50%	42%	0%
Federal Agencies __%	7	19	11
	15%	40%	23%
Private Agencies __%	28	9	1
	74%	24%	3%
Joint Agencies or Task Forces ___%	9	17	9
	20%	38%	20%
Other, ____%	19	5	2
	70%	19%	7%

13. My agency or organization has clear procedures/guidelines for reporting suspicious activity.

Strongly Disagree	1	2%
Disagree	2	4%
Agree	21	42%
Strongly Agree	26	52%
Total	50	100%

14. Clear, standard operating procedures have been established between public/private stakeholders.

Strongly Disagree	6	12%
Disagree	25	50%
Agree	18	36%
Strongly Agree	1	2%
Total	50	100%

15. What form of communication would be most effective for your organization to receive situational updates?		
Phone	29	58%
Fax	7	14%
Pager	2	4%
Email	40	80%
Online Website	10	20%
Other, please specify	5	10%

16. Approximate the percent of all terrorism awareness training you currently receive from each source			
Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option.	**0%**	**25%**	**50%**
Municipal __%	18 46%	15 38%	3 8%
County __%	21 57%	11 30%	1 3%
State __%	19 48%	11 28%	4 10%
Federal __%	6 12%	16 33%	12 25%
Private __%	19 46%	11 27%	6 15%
Other__%	20 69%	5 17%	0 0%

17. How do you rate your SATISFACTION with the level of terrorism training you receive to secure critical infrastructure?		
Very Dissatisfied	4	8%
Dissatisfied	28	56%
Satisfied	18	36%
Very Satisfied	0	0%
Total	50	100%

18. More terrorism/disaster preparedness training would benefit my organization.

Strongly Disagree	0	0%
Disagree	2	4%
Agree	20	40%
Strongly Agree	28	56%
Total	50	100%

19. My employment is primarily with an agency or organization at the following tier:

Municipal	17	34%
County	1	2%
State	0	0%
Federal	6	12%
Private	25	50%
Other, please specify	1	2%
Total	50	100%

20. My current discipline is best described as:

Law Enforcement/Government	24	48%
Private Security/Facility Security Officer	21	42%
Other, please specify	5	10%
Total	50	100%

21. Please add any additional comments or feedback.

22 Responses

22. (OPTIONAL) Please give me a little information about yourself. Again, individual results will remain confidential.
51 Responses

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. David Brannan
   Naval Post Graduate
   Monterey, California

4. Michael Grossman
   Los Angeles County Sheriff’s Department
   Los Angeles, California

5. Chief Anthony Batts
   Long Beach Police Department
   Long Beach, California